Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-19. (Canceled)

20. (Currently amended) A computer system having an input/output processing unit for executing a file access, an access execution unit for requesting a file access via the input/output processing unit in response to a user instruction, and an access control unit for performing access control when the file access is executed, wherein the access control unit comprises:

a storage unit protected from the access execution unit;

a file list stored in the storage unit describing security levels of files;

a user list stored in the storage unit describing clearances of users;

an access control processing unit for determining whether the file access is legal in accordance with the file list, the user list, an access type of the file access, information identifying a file, and information identifying a user, wherein if a host OS program of the access control processing unit is tampered with, a guest OS of the access control processing unit is instructed to invalidate one or more functions of the host OS program;

an enciphering unit for encrypting a file when storing the file on a storage medium;

a deciphering unit for decrypting the encrypted file when retrieving the encrypted file from the storage medium; wherein the storage unit stores at least one cipher key commonly used among a plurality of security levels for each file~~at least one key created independently of the user~~, ~~which~~ the encipher key ~~is~~ used for both encrypting and decrypting; and

an access monitor unit which:

when the input/output processing unit executes a file access, sends the access type, the information identifying the file, and the information identifying the user to the access control processing unit;

receives a validity determination result of the file access from the access control processing unit; and

if the file access is legal, causes the input/output processing unit to execute the file access, and if the file access is illegal, inhibits the file access.

21. (Previously presented) A system as in claim 20 further comprising an exclusive control unit for protecting, from the access execution unit, a storage area of the storage unit to be used by the access control processing unit.

22. (Previously presented) A system as in claim 21 further comprising a user list setting/managing unit for setting and managing the user list.

23. (Previously presented) A system as in claim 22 wherein the user list setting/managing unit includes an authentication unit for authenticating a security administrator.

24. (Previously presented) A system as in claim 23 wherein the security administrator is different from a system administrator who manages the access execution unit.

25. (Previously presented) A system as in claim 20 further comprising a file list setting/managing unit for setting and managing the file list.

26. (Previously presented) A system as in claim 25 wherein the file list setting/managing unit includes an authentication unit for authenticating a security administrator.

27. (Previously presented) A system as in claim 26 wherein the security administrator is different from a system administrator who manages the access execution unit.

28. (Previously presented) A system as in claim 20 further comprising:

an enciphering unit for encrypting a file if the file access requesting to output a file to the storage unit is legal; and

a deciphering unit for decrypting the enciphered file if the file access for requesting to input the enciphered file from the storage unit is legal.

29. (Previously presented) A system as in claim 28 wherein an exclusive control unit protects from the access execution unit a storage area in the storage unit storing at least one key information set to be used by the enciphering unit and the deciphering unit.

30. (Previously presented) A system as in claim 20 wherein the enciphering unit and the deciphering unit use a plurality set of different key information and at least one cipher method for each security level written in the file list.

31. (Previously presented) A system as in claim 20 further comprising an input/output monitor unit for monitoring that the input/output processing unit or the access monitor unit is not tampered or performs a predetermined operation, and instructing to inhibit an input/output of a file if the input/output processing unit or the access monitor unit is tampered or performs an operation different from the predetermined operation.

32. (Previously presented) A system as in claim 20 further comprising a file access log processing unit for storing and managing information on each file access sent to the access control processing unit.

33. (Previously presented) A system as in claim 20 wherein the access control unit is realized by a software module.

34. (Previously presented) A system as in claim 20 wherein the access control unit is realized by a hardware module.

35. (Previously presented) A system as in claim 20 wherein the key comprises a symmetric key.